Consent Options for Electronic Health Information Exchange in Texas

Patricia Gray, J.D., LL.M.

UNIVERSITY of HOUSTON | LAW CENTER

Health Law & Policy Institute

Prepared for the Texas Health and Human Services Commission and the Texas Health Services Authority with support from the State Health Information Exchange Cooperative Agreement Program

June 2011

CONSENT OPTIONS FOR ELECTRONIC HEALTH INFORMATION EXCHANGE IN TEXAS

TABLE OF CONTENTS

Executive Summary……3

Introduction……5

Application of state and federal laws and regulations……6

Defining consent and authorization in an HIE……9

Consent and data segmentation……12

- **A. Core consent models……13**
- **B. Data segmentation ……16**
- **C. Special issues: Secondary uses of PHI……17**

Key Policy Questions……18

Conclusion……21

CONSENT OPTIONS FOR ELECTRONIC HEALTH INFORMATION EXCHANGE IN TEXAS

EXECUTIVE SUMMARY

One of the biggest challenges in the development of an electronic health information exchange (HIE) is how to address the role of consent for patient participation in the exchange. Consumer studies have consistently shown that patients see the use of interoperable electronic health records as beneficial, but have concerns about the use of their data without their permission for activities not directly related to their treatment.[1] A tradeoff exists between patient control and the completeness and value of electronic health records. Consent and authorization protocols that include a range of options may successfully manage this tradeoff while encouraging patient participation and trust.

Both federal and Texas law support the exchange of health data through electronic networks and together govern the use and disclosure of health care data once it is in an exchange. However, neither requires that patients consent in advance to participation in an exchange.

Texas has an expanded definition of "covered entity" that incorporates not only "covered entities" as defined under HIPAA, but any other entities or individuals who obtain, store, transmit or otherwise use protected health information (PHI) and their employees, agents or contractors.

Consent and authorization may have specific meanings when used in the context of medical information privacy laws. The Privacy Rule uses the term **consent** to describe permission that is not required but that may be obtained from an individual prior to using or disclosing that individual's PHI. The Privacy Rule uses the term **authorization** to refer to permission that is required from an individual by a health care provider to disclose the individual's PHI for purposes other than treatment, payment, and health care operations. Rules governing use or disclosure of federally funded substance abuse treatment (commonly called Part 2 rules) are more stringent than the Privacy Rule and use the term consent in the way that authorization is defined by the Privacy Rule.

For this paper, consent is used in the context of the patient's permission for inclusion of their PHI in an HIE. There are five generally accepted models for defining patient consent to participate in an HIE. The **no-consent** model does not require any agreement on the part of the patient to participate in an HIE. The **opt-out** model allows for a pre-determined set of data to be automatically included in an HIE but a patient may still deny access to information in the exchange. The **opt-out with exceptions** model allows a patient's PHI to be made available in an

[1] Markle Foundation, *Survey finds Americans Want Electronic Personal Health Information to Improve Own Health Care,* Nov., 2006, *available at* http://www.markle.org/downloadable_assets/research_doc_120706.pdf. Posted by stevegonhit, *Health IT privacy focus turns to patient consent,* April 26, 2010, *available at* http://searchhealthit.techtarget.com/healthitexchange/hitseccurityandprivacy/health-privacy-focus

exchange but enables the patient to selectively exclude data from an HIE, limit information to specific providers, or limit exchange of information to exchange for specific purposes. The **opt-in** model requires patients to specifically affirm their desire to have their data made available for exchange within an HIE. The **opt-in with restrictions** model allows patients to make all or some defined amount of their data available for electronic exchange.

The process for limiting access to or disclosure of parts of a patient's data is commonly referred to as data segmentation. Data segmentation is defined as the process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution, organization, or individual as being undesirable to share. Patients, providers and payers have different views about whether and how much data segmentation should occur in an HIE.

Patients' concerns about secondary uses of their PHI may include medical research, public health surveillance, compilation of health information for inclusion in registries, and marketing.

Texas will need to consider policies that address patient control of information, risk management, and feasibility of implementation of privacy protections to ensure compliance with state and federal laws and to ensure patient confidence in the security and privacy of their health information.

CONSENT OPTIONS FOR ELECTRONIC HEALTH INFORMATION EXCHANGE IN TEXAS

...if we are to reap the benefits of information exchange, patients must be assured that appropriate...policy protections will be employed to prevent their information from being used in undesirable ways or to generally impinge upon their rights...[2]

INTRODUCTION

Key Points

- Studies show that consumers see the benefit of interoperable electronic health records but are concerned about the use of their personal health information.
- A tradeoff exists between patient control and the completeness and value of electronic health records.
- Consent and authorization protocols that include a range of options may successfully manage this tradeoff while encouraging patient participation and trust.

The ability to access relevant patient information through interconnected and searchable electronic health records represents an opportunity to improve the quality of patient care while reducing waste and inefficiency in health care delivery and to enhance medical research options to improve general medical knowledge.[3] One of the biggest challenges in the development of an electronic health information exchange (HIE) is how to operationalize the role of consent for patient participation in an exchange. Patients, providers, and HIE administrators will have different views about how an HIE should function.[4] As Texas moves forward with development of HIE networks, achieving the essential goal of ensuring patient participation hinges, in part, on whether patients are comfortable with the ways that their individually identifiable protected health information (PHI) might be used once it is in an exchange network. Consumer studies have consistently shown that patients see the use of interoperable electronic health records as beneficial but are concerned about misuse of their personal information.[5]

The use of patient consent protocols may help to alleviate some patient concerns, but only if the

---

[2]Melissa M. Goldstein and Alison L. Rein, *Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis*, March 23, 2010 Executive Summary, p. 1 *available through* http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_home/1204 (search consent options) hereinafter C*onsumer Consent Options*.

[3] *See generally*, Mark A. Hall, *Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records*, 95 IOWA L. REV. (Feb. 2010).

[4] Kristen Rosati, *Consumer Consent for Health Information Exchange: An Exploration of Options for Arizona's HIEs, Arizona eHealth Connection* at 2.

[5] Markle Foundation, *supra*, note 1.

protocols have a sufficient range of options to allow patients to maintain an appropriate level of control over the information made available through an exchange. Allowing too much patient control can result in an incomplete health record in the exchange that may diminish the effectiveness of a patient's care and other useful aspects of patient information, such as data aggregation for medical research or public health surveillance. Allowing too little control, however, may result in a lack of patient trust and diminish patient participation.

Giving patients the ability to segment their data based on their consent and authorization, though technically challenging, represents an avenue toward striking a balance between the two extremes.

The purpose of this paper is to discuss the policy issues related to achieving the balance between ensuring patient privacy and maximizing the utility of data shared through an HIE by examining the role that patient consent for participation in an HIE plays in achieving that balance.

APPLICATION OF STATE AND FEDERAL LAWS AND REGULATIONS

Key Points

- Texas has an expanded definition of covered entities that includes health plans, health care clearinghouses, health care providers, business associates, and employees, agents, and contactors who obtain, store, transmit or use patients' health information.
- Regulatory gaps, inconsistencies, and differing levels of stringency require HIE policy makers to assure patients that their privacy concerns are being addressed.
- The two primary gaps in existing regulation are i) regulation of entities that are not defined as covered entitles but may legitimately seek to access PHI from an HIE for a beneficial purpose and ii) reimbursement to an HIE for release of PHI.

The terms "consent" and "authorization" are often used interchangeably when referring to patient permission to take or not take an action, but these terms can have specific definitions and applications under both state and federal laws and regulations. The primary federal regulation governing medical information privacy is the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,[6] which was recently amended and strengthened by the Health Information Technology for Economic and Clinical Health Act (HITECH).[7] HITECH also encourages state initiatives to develop electronic health information exchanges by making grants available to states for that purpose. Under both HIPAA and HITECH, states have considerable flexibility to create models that will add value and improve health care for their populations.

[6] Health Insurance Portability and Accountability Act of 1996 (HIPAA) Pub. L. No. 104-191 (1996), *codified in* 45 C. F. R. Pts. 160, 162 and 164.

[7] American Recovery and Reinvestment Act of 2009 (ARRA), Publ. L. 111-5 (2009) (*enacted as* The Health Information Technology for Economic and Clinical Health Act (HITECH) *in* Title XIII Div. A and Title IV Div. B).

The Privacy Rule regulates PHI that is in the possession of specifically defined "covered entities"[8] and PHI that third parties use for or on behalf of those covered entities through business associate agreements.[9] The Privacy Rule defines "covered entities" as health plans, health care clearinghouses, and health care providers.[10] HITECH brought business associates under the enforcement provisions of HIPAA.[11] Texas has an expanded definition of "covered entity" that incorporates not only "covered entities" as defined under HIPAA, but any other entities or individuals who obtain, store, transmit or otherwise use PHI, and their employees, agents or contractors.[12]

The Privacy Rule requires appropriate safeguards to ensure the privacy of individuals' PHI, setting limits and conditions on the uses and disclosures that may be made of such information without specific patient concurrence.[13] The Privacy Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records,[14] and to request corrections to their health information.[15] Other federal statutes,[16] including those authorizing the Medicare, Medicaid and State Children Health Insurance programs, also govern the privacy of PHI.

Statutes sometimes use the phrase "or as authorized by law" when referencing circumstances under which PHI may be disclosed. This phrase incorporates the regulations developed to implement legislation, including the regulations developed pursuant to HIPAA and HITECH. These regulations add detail to what is required when implementing statutes.

Texas, like many states, has its own laws that protect the privacy of an individual's medical information. In Texas, such provisions are found primarily in the Occupations Code (Texas Medical Practice Act)[17] and the Health & Safety Code (Texas Medical Records Privacy Act),[18] but can also be found in other codes as well as in the Texas Administrative Procedures Act and in case law.[19]

---

[8] 45 C. F. R. §160.102.
[9] Bernstein, *et al*., *supra* note 4.
[10] 45 C. F. R. §160.102 and 160.310.
[11] HITECH §13404.
[12] TEX. HEALTH & SAFETY CODE ANN. § 181.001(b)(2).
[13] The Privacy Rule requires a covered entity to make reasonable efforts to use, disclose and request only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request. *See* 45 C. F. R. §164.502(b) and §164.514(d).
[14] 45 C.F.R. §164.524.
[15] 45 C.F.R. §164.526.
[16] *See generally* the Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, 122 Stat. 881 (2008); the Family Educational Rights and Privacy Act; the Clinical Laboratory Improvement Act; 42 C. F. R. Pt 2.
[17] TEX, OCC. CODE §159.001, *et seq*.
[18] TEX.HEALTH & SAFETY CODE §§181.001- .181.205.
[19] *See generally*, Texas Primer on Medical Information Privacy, available at http://www.thsa.org/media/1812/primer_medical_information_privacy-protections_texas_3-15-2011.pdf.

Texas laws are sometimes more stringent than the Privacy Rule, but these laws, like those in other states, have been developed primarily under a paper-based system in which health care providers and insurers are the primary possessors of patients' health care information.[20] Thus Texas medical information privacy laws are basically structured around the types of entities that have historically maintained and transmitted medical information. [21] However, in 2009, the Texas Legislature adopted House Bill 1218 directing the Texas Health & Human Services Commission to establish an electronic health information exchange pilot project in at least one urban area, including participation from at least two local or regional health information exchanges in order to assess the feasibility, costs and benefits of electronic HIE. The bill also set out the requirements for implementing the HIE but did not specifically address consent and authorization issues.[22] In 2011, the Texas Legislature adopted HB 300 which requires that covered entities provide notice if a consumer's PHI is subject to electronic disclosure, and that authorization be obtained for any disclosure not related to "…treatment, payment, health care operations, or…as otherwise authorized or required by state or federal law."[23]

Several reports from within Texas[24] and from national study projects[25] have identified gaps in regulation, inconsistencies in terminology, differing levels of stringency related to privacy of health information, and tensions between provisions of existing statutes that will impact design and implementation of HIE networks. [26] For example, the Privacy Rule governs disclosure of PHI by covered entities, [27] but HIEs are generally not considered covered entities under HIPAA, though they may be a business associate of a covered entity and thus subject to the same requirements of protecting PHI under HIPAA.[28] However, HIEs likely fall under the definition of a covered entity under Texas law, and thus are subject to requirements of the Privacy Rule as implemented under Texas law. In addition, the patient data exchange envisioned through an HIE may include activities for which specific patient authorization may or may not be required, depending on state statute or regulation. A 2004 comprehensive analysis of Texas statutes conducted by the Office of the Attorney General found many provisions of state law related to use and disclosure of PHI that were in tension with provisions of the Privacy Rule, but none were specifically "contrary" to the Privacy Rule so as to trigger analysis of whether the Privacy Rule

---

[20] Bernstein, *et al.*, *supra* note 4.
[21] Texas Primer on Medical Information Privacy, *supra* note 19.
[22] *Codified in* TEX. GOV. CODE ANN. §531.901-513.913.
[23] HB 300, 82nd Texas (R) at SECTION 7, §181.154.
[24] Report of the Off'c of the Att'y Gen. of Texas, *Preemption Analysis of Texas Laws Relating to Privacy of Health Information and the Health Information and Portability and Accountability Act and Privacy Rules (HIPAA),* November 4, 2004 *available at* http://www.oag.state.tx.us/notice/hipaa.pdf.
[25] *See generally* The Health Information Security and Privacy Collaboration (HISPC) *available at* http://HealthIT.hhs.gov/HISPC.
[26] NCVHS, Letter to the Secretary of Health and Human Services re: *Update to privacy laws and regulation required to accommodate NHIN data sharing practices*, June 21, 2007, *available at* http://www.ncvhs.hhs.gov.
[27] 45 C.F. R. §164.502 and §164.506.
[28] *See* http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/introduction.pdf.

would or would not pre-empt the Texas statute.[29] (It should be noted that this preemption analysis has not been updated to consider whether provisions of Texas law are still in tension with HIPAA's Privacy Rule as expanded by the HITECH provisions of 2009.)

Patients frequently assume that the privacy protections afforded through state and federal regulatory mechanisms are sufficient to ensure their personal control over disclosure of their PHI. However, the technology for implementing electronic exchange of information, as well as gaps in the regulatory schemes governing health information privacy, require policymakers to confront the questions that patients may be unable to articulate on an individual basis in order to assure patients that their privacy concerns are being addressed.

Two themes emerge as the most common concerns about gaps in the regulatory process. The first centers around governance of entities that do not fall under the definition of a covered entity but that may legitimately seek to access PHI from an HIE for beneficial purposes, such as the Red Cross, which may seek to gather health data to provide assistance in the event of a natural disaster, or companies that provide support to covered entities' information management systems. The second major area of concern is related to reimbursement to covered entities for release of PHI. The 82nd Texas Legislature adopted HB 300, which authorizes reimbursement to a covered entity for release of PHI only for purposes of treatment, payment, health care operations,…or as "otherwise authorized or required…by state or federal law."[30]

DEFINING CONSENT AND AUTHORIZATION IN AN HIE

Key Points

- The Privacy Rule uses the term **consent** to describe permission that is not required but that may be obtained from an individual prior to using or disclosing that individual's PHI.
- The Privacy Rule uses the term **authorization** to refer to permission that is required from an individual by a health care provider to disclose the individual's PHI for purposes other than treatment, payment, and health care operations.
- Rules governing use or disclosure of federally funded substance abuse treatment (commonly called Part 2 rules) are more stringent than the Privacy Rule and use the term consent in the way that authorization is defined by the Privacy Rule.
- For this paper, consent is used in the context of the patient's permission for inclusion of their PHI in an HIE.

Understanding the definitions of "consent" and "authorization" as set forth in the Privacy Rule is particularly important when considering how to secure patient information in an HIE. The

[29] Report of the Off'c of the Att'y Gen. *supra* note 24.
[30] HB 300, 82nd Texas (R), SECTION 7, §181.153.

Privacy Rule generally uses the term "consent"[31] to describe permission that is *not required*, but that may be obtained from an individual prior to using or disclosing that individual's PHI. Certain disclosures are permitted without requiring additional authorization. For example, authorization is not required from an individual for purposes related to treatment of the individual (such as obtaining an X-ray), obtaining payment for services rendered to the individual (such as billing the patient's insurer), or for health care operations of the entity (such as monitoring the quality of services rendered).[32] Additionally, authorization is not required for certain other disclosure as specified in the Privacy Rule, including public interest and benefit activities.[33] However, a covered entity could choose to obtain consent for such disclosures. Consent under the Privacy Rule is not the same as the "informed consent" for treatment that a provider obtains from a patient before instituting medical care; rather it is consent to use information that is available in a patient's health record or to disclose certain information from that record for certain purposes as set forth in the Privacy Rule.[34]

The Privacy Rule uses the term "authorization" to refer to the permission that is *required* from an individual by a health care provider to disclose the individual's PHI for purposes other than those exceptions defined in HIPAA. An authorization may limit the amount of PHI a health care provider may release to that which is relevant to the purpose of the disclosure, and it may also limit who is authorized to access the PHI.[35] As mentioned earlier, Texas law imposes more stringent requirements than does the Privacy Rule for disclosure of PHI in some instances, though its terminology for approving that disclosure is inconsistent.[36]

A separate set of federal rules related to disclosure of information about an individual's substance abuse diagnosis and treatment uses the term consent in the same way the Privacy Rule uses the term authorization. These rules, commonly referred to as Part 2 requirements because they are found at 42 C.F. R. Part 2, are much more stringent than the Privacy Rule. Requirements for a valid Part 2 consent include several limiting elements such as a specified date, event or condition triggering expiration of the consent that, if omitted, invalidate the consent.[37] There are also limitations on exchange of such data through an electronic HIE. The HIE must enter into a Qualified Service Organization Agreement (QSOA) with a qualified provider covered under Part 2 in order to receive a patient's PHI, including accepting such data

---

[31] *See, e.g.* HHS, *Health Information Policy: What is the Difference Between "Consent" and "Authorization" Under the HIPAA Privacy Rule?* March 14, 2006, *available at* http://www.hhs.gov/ocr/privacy/hipaa/faq/authorizations/264.html.

[32] *See generally* 45 C.F.R. §164.502.

[33] For a more comprehensive discussion of the circumstances under which consent is not required, *see generally*, Texas Primer on Medical Information Privacy, *supra* note 19.

[34] HHS, *supra* note 31.

[35] 45 C.F.R. §164.508.

[36] Texas' terminology for consent and authorization includes "consent", "consent form", "release", "written release" and "written consent".

[37] 42 C.F.R. §2.11 and 2.13.

for treatment, payment and health care operations.[38] A QSOA only allows for exchange of information between the HIE and qualified treatment providers. Additional written patient consent (authorization) is required in order for any provider or entity not covered by the QSOA to access the information.[39]

For purposes of this paper, the term consent is used in the context of the patient's permission for inclusion of their PHI in an HIE and the implications of obtaining or not obtaining that consent. The Office of Civil Rights, the entity charged with primary enforcement of the Privacy Rule, has given some guidance on the subject of whether or not patients must give advance consent for participation in an HIE, concluding that the Privacy Rule does not require that advance consent be obtained.[40] However, both the Privacy Rule and state law provide a basis of support for an individual's decision to make choices about the collection, use, and disclosure of their PHI.[41] Analysis of consent options related to patients' participation in electronic exchange of health information centers around whether patients will be given, either through federal or state-level policy or through individual HIE policy direction, the option to consent to participate in the exchange, whether patients will be given options to control the content or completeness of their health information that is included in an exchange, and the method of control patients may exercise over how their health information in the exchange is accessed and used.[42] As the number of exchanges increases, these issues will likely gain more attention. A recent eHealth Initiative survey reports that there were 73 operational exchanges transmitting data at the end of 2010 in the United States.[43] At that point in time, only thirteen of those exchanges had actually instituted policies addressing patients' ability to participate in determining individual data elements for the exchange of their information, though more than half allowed patients to view their data and about one-third allowed patients to contribute information about their health status.[44]

---

[38] *Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange: Frequently Asked Questions*, at p. 6, *available at* http://www.samhsa.gov/HealthPrivacy/docs/EHR-FAQs.pdf.
[39] 42 C. F. R. §2.31.
[40] *See* http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/individualchoice.pdf.
[41] *Id.*
[42] NCVHS, Ltr to the Sec'y of Health and Human Servs., *Privacy and Confidentiality in the Nationwide Health Information Network,* June 22, 2006, *available at* http://www.ncvhs.hhs.gov/060622lt.htm.
[43] *The State of Health Information Exchange in 2010: Connecting the Nation to Achieve Meaningful Use* at 2 *available at* http://www.ehealthinitiative.org/uploads/file/Final%20Report.pdf.
[44] *Id.* at 3

CONSENT AND DATA SEGMENTATION

Key Points

Consent Options

- The **no-consent** model does not require any agreement on the part of the patient to participate in an HIE.
- The **opt-out** model allows for a pre-determined set of data to be automatically included in an HIE but enables a patient to deny access to information in the exchange.
- The **opt-out with exceptions** model allows a patient's PHI to be made available in an exchange but enables the patient to selectively exclude data from an HIE, limit information to specific providers, or limit exchange of information to exchange for specific purposes.
- The **opt-in** model requires patients to specifically affirm their desire to have their data made available for exchange within an HIE.
- The **opt-in with restrictions** model allows patients to make all or some defined amount of their data available for electronic exchange.

Data Segmentation

- Data segmentation is defined as the process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution, organization, or individual as being undesirable to share.
- Patients, providers and payers have different views about whether and how much data segmentation should occur in an HIE.

Special Issues: Secondary Uses of PHI

- Secondary uses of PHI may include medical research, public health surveillance, compilation for inclusion in registries, and marketing.

Two recent papers prepared for the Office of the National Coordinator for Health Information Technology (ONC) by Melissa Goldstein, a physician at the George Washington University Medical Center, and Alison Rein, Director of Academy Health, help delineate some of the policy issues that must be considered related to the level of control patients may use governing access to and use of their individual PHI in an HIE. The first paper defined five core consent models governing the ability of patients to control whether their PHI may be submitted for use in an HIE.[45] Examination of these core models is useful because the models help differentiate the

[45] *Consumer Consent Options*, *supra* note 2.

concerns of providers and patients. The second paper prepared for the ONC focused on clarifying issues regarding the degree of control patients should have to segment their data in order to limit access to and use of their PHI in an HIE and the implications that various levels of such control have on design and implementation of an HIE.[46]

A. CORE CONSENT MODELS

Both federal and state law support the exchange of health data through electronic networks, but neither federal nor Texas law requires that patients consent in advance to participation in an exchange. As other states have examined the desirability as well as the feasibility of obtaining advance consent, certain core models have emerged defining advance consent options.

The five core consent models identified by Goldstein and Rein are: (1) no-consent; (2) opt-out; (3) opt-out with exceptions; (4) opt-in; and (5) opt-in with restrictions.[47] The authors concluded that, in practice, it would be difficult to implement any of the core models in isolation.[48] As indicated in the following discussion, some states have chosen to implement hybrids of these models.

The *no-consent* model does not require any agreement on the part of the patient to participate in an HIE. However, a *no-consent* requirement to participate in the electronic HIE does not abrogate the requirements of federal and state privacy laws governing the terms of access to a patient's medical information. The *no-consent* model generally addresses concerns by providers that missing or incomplete information in an electronic exchange can result in diminished quality of care for a patient. Both Indiana and Delaware authorized HIEs in their states to adopt *no-consent* policies, though both have effectively implemented hybrid models in that they allow for a patient to deny access to all information in the HIE if they so choose, even though the data stays in the exchange. In addition, neither Indiana nor Delaware accept information related to federally funded treatment of alcohol and substance abuse for inclusion in their HIEs due to the stringent consent and authorization requirements for disclosure of this information.[49] The advantages of a *no-consent* model are the increased amount of information available for exchange within an HIE, the flexibility it provides in coordinating with other HIEs and its ease of administration since it does not involve implementation of an opt-in or opt-out process.[50] Unanswered questions concern how much notice must be given to patients about the fact that their PHI is being submitted to an HIE, who will give the notice, and how an HIE that uses a *no-*

---

[46] See generally, Melissa M. Goldstein and Alison L. Rein, *Data Segmentation in Electronic Health Information Exchanges: Policy Considerations and Analysis* (September 29, 2010) *available through* http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_home/1204 (search data segmentation) hereinafter *Data Segmentation*.
[47] *Consumer Consent Options*, *supra* note 2.
[48] *Id.*
[49] *Id.*
[50] Rosati, *supra* note 4 at 7.

consent model can interface with an HIE that requires stringent consent for participation.[51] The primary disadvantage of the *no-consent* model is the lack of patient control, especially for patients who are particularly concerned about control of sensitive information[52] in their PHI.[53]

The *opt-out* model allows for a pre-determined set of data, such as lab results, imaging, or hospital discharge summaries, to be automatically included in an HIE, but enables any patient to deny access to the information in the exchange. Delaware combines its *no-consent* model with a patient opt-out provision. Under Delaware's hybrid model, patient information is sent to the exchange, but patients may opt out of allowing access to their information by filing a written request to block all access to their information. The block will deny access even in emergency situations. A pure *opt-out* model does not allow for exceptions. A patient either acquiesces to allowing access to the information in the exchange or opts out completely. Other applications of *opt-out* models are found in Virginia and Tennessee, both of which have procedures for removal of data for patients who opt out.[54] In addition, like Indiana and Delaware, neither Virginia nor Tennessee store sensitive information. The *opt-out* approach satisfies some patient concerns about having personal health information in an exchange, but it also denies patients an ability to benefit from participation because of its all-in or all-out design.[55] There are also challenging operational issues in implementing such a model: (a) Who will collect the necessary information for patients to opt out? (b) How will the opt-out information be communicated to the HIE and to other providers? (c) What processes can be implemented to handle cases where a patient changes his mind?[56]

An *opt-out with exceptions* model allows a patient's PHI to be made available in an exchange, but enables the patient to selectively exclude data from an HIE, limit exchange of information to specific providers, or limit exchange of information to exchange for specific purposes.[57] This model gives patients more control over the exchange of their PHI, but is seen by many as the most difficult approach to implement from a technical standpoint.[58] Minnesota, for example, allows for patient information to be included in an electronic record locater service (RLS). An RLS is an electronic index of patient identifying information that directs providers to the location of the patient's records. Patients can opt out of having their identifying information in the RLS,

---

[51] *Id.*
[52] Sensitive information is broadly defined as that which is granted special privacy protection in either statute or regulation, such as test results for sexually transmitted disease, treatment for mental illness or substance abuse, or genetic information, as well as information that the patient deems too personal to be shared unless absolutely necessary for his or her care, such as injuries suffered as a result of criminal assault. The Privacy Rule does not distinguish between data that is accorded special protection through statute and other data that an individual may designate as sensitive.
[53] Rosati, *supra* note 4 at 7.
[54] *Consumer Consent Options*, *supra* note 2.
[55] *Id.*
[56] Rosati, *supra,* note 4 at 6.
[57] Id.
[58] *Consumer Consent Options*, *supra* note 2.

or they may exclude certain providers from accessing their identity in the RLS.[59] The administrative challenges to implement this model are similar to that of the *opt-out* model.

At the other end of the spectrum of core consent models are *opt-in* and *opt-in with restrictions*. In the *opt-in* model, patients must specifically affirm their desire to have their data made available for exchange within an HIE. As with the *opt-out* model, participation is on an all-in or all-out basis.[60] The appeal of an *opt-in* model is that it gives patients up-front control over whether they will participate or not. Since an *opt-in* model requires specific patient consent, it also provides an opportunity for patient education on the advantages and disadvantages of participation. An *opt-in* approach may also enable better record matching between patients and their data because the process of obtaining advance consent could incorporate collection of secure identifiers such as biometric identifiers.[61] Disadvantages of the *opt-in* model are primarily the administrative complexity of implementing such an approach: (a) Who will obtain the consent? (b) Will one consent suffice for participation in the system as a whole or must each provider obtain consent for his or her own patients? (c) What process will be used to communicate the patient's consent? (d) What happens if a patient wants to withdraw his consent? Can his data be removed from the HIE or will the withdrawal of consent only be effective for data developed after the withdrawal of consent was given?[62]

Opt-in with restrictions allows patients to agree to make all or some defined amount of their data available for electronic exchange. Patients may restrict how their data is used by allowing access only to specific providers, by allowing only specific data elements to be included, or by allowing data to be accessed only for specific purposes.[63] Exchanges in New York and Massachusetts utilize an *opt-in* approach to patient consent, while Rhode Island uses an *opt-in with restrictions* approach.[64]

It should be noted that actual implementation of the consent models referenced above is still in early stages of development. The analyses are largely theoretical. It appears that each HIE or HIE network can develop its own model of consent for patient participation, raising the issue of how HIEs with different consent options will interface with each other and maintain patient confidence.

Determining which of the core consent models might be adapted for use in Texas on a statewide basis or by individual HIEs also requires consideration of the number of entities participating in an exchange, the types of information included in the exchange, how information in the

---

[59] *Health Information Technology and States: A Project Report from NCSL's Health Information Technology Champions* (February 2009) at p. 9. It should be noted that some privacy advocates object to Record Locater Services or Master Patient Indexes because disclosing the location of a patient's record can be used to identify patients who may have been treated for illnesses that fall under the definition of sensitive health information.
[60] *Consumer Consent Options*, *supra* note 2.
[61] Rosati, *supra* note 4 at 4-5.
[62] Rosati, *supra* note 4 at 6.
[63] *Id.*
[64] *Id.*

exchange may be secured, and the remedies available to patients in the event information is wrongfully accessed or released.[65] The decisions that result from such an assessment will impact the technological implementation of an HIE, as certain levels of consent and authorization may prove too difficult or too costly to implement.[66]

B. DATA SEGMENTATION

Patients' desires to control the privacy of their health data, together with state and federal medical information privacy laws and regulations, are driving the current focus on what is referred to as data segmentation of health information.[67] Data segmentation is defined by Goldstein and Rein as the process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution, organization, or individual as being undesirable to share.[68] In the case of health information, some patients may prefer to withhold or sequester certain elements of their medical record, often when it is deemed by them to be sensitive, whereas others may feel comfortable that all of their health information should be shared in order to enhance their medical care.[69] Giving patients finely detailed granular choices about what data may be shared with whom and for what purposes means that data may be segmented in myriad ways.

Patients, providers and payers have different concerns about the use of health information that highlight the importance of data segmentation. As Lee Barrett, Executive Director of the Electronic Healthcare Network Accreditation Commission notes, "Payers want to reduce costs, providers want to improve the quality of care and have easy access to information and patients still want some control over who is accessing the information. We need to be aware that all of these stakeholders have different objectives, and we need to be able to manage those objectives."[70]

Providers generally want all of the clinical data available for a particular patient in order to ensure high quality care and, perhaps, to diminish liability concerns. Segmenting data to limit disclosure may limit critical information for the physician and may also stymie adequate coordination of care between different types of providers.[71] However, some physicians, particularly those who provide treatment for sensitive conditions such as substance abuse or

[65] Rosati, *supra,* note 4 at 6.
[66] Rosati, *supra* note 4 at 2.
[67] *Data Segmentation, supra* note 46 at 10.
[68] *Data Segmentation, supra* note 46 at ES-1.
[69] *Id.*
[70] Quoted in Lisa A. Eramo, *Permission Predicament,* For the Record, 22:17 at 24 (Sept. 13, 2010).
[71] *Data Segmentation*, *supra* note 46 at ES-1.

mental illness, argue that limiting patients' ability to consent to participate in an HIE and to control access to their PHI may discourage some individuals from seeking treatment at all.[72]

Patients who see the possibility of enhanced communication between their providers and better coordination of their care may be less concerned about giving advance consent.[73] Other patients, however, may want to limit access to their PHI only to those who need access to participate in the patient's treatment, and only for the time necessary to carry out the treatment. Patients also have concerns about sensitive data that historically has been used to deny insurance coverage or limit job access, that might impact their personal safety if disclosed, as in the case of crime victims, or that might simply be embarrassing if disclosed. Certain categories of information such as genetic information[74] or treatment for such maladies as substance abuse and alcoholism, HIV, sexually transmitted diseases, mental illness and sickle cell anemia are afforded special privacy protections in both federal and state statutes. The National Committee on Vital and Health Statistics (NCVHS) includes treatment related to domestic violence and reproductive health in its delineation of sensitive information.[75] Minors also have the right to limit access to their PHI under certain conditions.[76] Failure to address legitimate issues about managing these and other concerns could prevent the full realization of the benefits of electronic exchange of health information.

C. SPECIAL ISSUES: SECONDARY USES OF PHI

Patients have a particular concern about secondary uses of their PHI for activities such as medical research, public health surveillance, compilation for inclusion in registries and, especially, sale or marketing of their PHI.[77]

Some patients may be supportive of allowing their PHI to be de-identified [78] and used for medical research, even if their PHI may subsequently be re-identified. However, even when patients are willing to have their PHI used for research purposes, they want to be informed about the purpose of the research and are more likely to withhold consent for research that seems focused on developing commercial applications that inure to the benefit of the requestor and not to advance general medical knowledge.[79] At least one commentator has proposed that patients'

---

[72] Rosati, *supra* note 4 at 3.
[73] *Id.*
[74] Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, 122 Stat. 881 (2008).
[75] NCVHS, *Letter to the Secretary of Health and Human Services re: Individual Control of Sensitive Health Information via the Nationwide Health Information Network for Purposes of Treatment,* Feb. 20, 2008, at 2; available at http://www.ncvhs.hhh.gov/080220lt.pdf.
[76] 45 C.F. R. 164.502(g)(2) and (3).
[77] Markle Foundation, *supra* note 1.
[78] See 45 C.F.R. §164.514(a) and (b) and §45 C.F.R. 164.502(d).
[79] NCVHS Draft Document, Report to the Sec. of Health and Human Services re: *Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically collected and Transmitted Health Data,* at p. 6 (Oct. 21, 2007).

PHI in electronic HIEs be used only for non-proprietary purposes,[80] though this could arguably limit access for some medical research.

Public health data may also be collected in local, state and federal agencies using a variety of mechanisms, and the ability to tap into large data bases of patient PHI that may be generated in HIEs may present some unanticipated concerns about how that data might be used, even if the initial intended use has a clear public health purpose.[81] Public health surveillance has moved beyond reporting disease outbreaks. A project in New York was designed to capture blood test levels from diabetes patients with the intent to contact the patients individually about potential improvements in diabetes management.[82]

Finally, patients have a particular concern about possible sale of their PHI, even if such data is sold in a de-identified format or the "sale" is in actuality a reimbursement to a provider for the cost of gathering and transmitting the data for beneficial activities such as for approved research projects.[83] The underlying issue of why sale of any data would be offered relates to the financial sustainability of HIE networks. Sale of data is obviously not the only way HIE networks might be financially sustained. User fees from participants, grants and taxpayer support may all be part of the mix for economic support of such networks. Although the Privacy Rule, particularly as amended by the provisions of HITECH, strengthens the prohibitions on sale of PHI by spelling out in more detail if and when exceptions to such sales require patient approval, such sales are not banned outright.[84]

KEY POLICY QUESTIONS

Goldstein and Rein formulated some fundamental policy questions based on their review of several states' proposed HIE implementation plans:[85]

(1) At what level is patient information blocked? Is information in the exchange in a view-only mode, unable to be modified or copied, and potentially limited in use to treatment of the individual patient or is the information in a computable form that can be incorporated into other data repositories and utilized for purposes other than treatment of the individual patient?

(2) Who determines the rules and protocols for sharing a patient's PHI? How will the individual patient's desires for privacy and control of PHI be balanced against the business practices and reporting requirements governing health care institutions and health information organizations?

---

[80] Sean T. McLaughlin, *Pandora's Box: Can HIPAA Protect Privacy Under a National Health Care Information Network?* 42 GONZ. L. REV. at 41.
[81] NCVHS, *supra* note 80 at 13.
[82] *Id.*
[83] *Id.* at 14.
[84] HITECH Act, §13405(d).
[85] *Data Segmentation, supra* note 46.

(3) Who has the authority or, perhaps more importantly, the ability to implement patient's choices?

The Statewide Health Information Exchange implementation plan for Texas states that Texas "could …adopt a consent policy to add an additional layer of patient protection and control" [of their PHI].[86] Texas HIE planners and policy-makers will have the opportunity to develop policies to address key policy questions in a number of areas relating to patient consent. At a high-level, one of the most significant questions will be whether the HIE proceeds under an "opt-in" or an "opt-out" consent model. Whichever model is chosen, a number of practical operational questions must be answered.

Operationalizing an "Opt-In" Consent Policy

- What will an opt-in requirement actually mean?
- Will patients be given options to consent to inclusion of data only for treatment and claims processing purposes, or will the opt-in consent cover other purposes authorized by law such as limited data sets for research purposes that are subject to a use agreement?
- If the choice is to simply allow patients to opt in, will one consent to participate suffice?
- If one consent is sufficient, how will that consent be communicated to other providers of the patient?
- Alternatively, if a patient has more than one provider, must each provider obtain the patient's consent to participate, and how will each provider's consent be communicated to other providers?

Operationalizing an "Opt-Out" Consent Policy

- What will an opt-out requirement actually mean? Will data be included in the HIE for purposes authorized by HIPAA, such as emergency access, public health surveillance, law enforcement purposes, or limited data sets for research purposes that are subject to a use agreement?
- Will a patient be required to opt-out at each encounter?
- How will a patient's decision to opt-out be communicated to interested parties (including, but not limited to providers)?
- What foreseeable consequences will opting-out have on the patient, provider, and delivery of care?

[86] State of Texas *Strategic and Operational Plans for Statewide Health Information Exchange* §16.2

Withdrawal of Consent

- How will withdrawal of consent be managed?
- If a patient withdraws consent to exchange data through an HIE, must all of the data currently aggregated by any participant in the HIE be withdrawn?
- If so, what proof that such withdrawal has occurred will suffice?

Granular Control

- If patients are allowed to opt-in with restrictions on what data is transmitted through an exchange as well as who can access such data, how will these restrictions be communicated to other participants?
- How will the restrictions be monitored to ensure compliance with the patient's request?
- What remedies will be available to patients whose restrictions are not followed?

Minors and Consent

- How will consent from minors be obtained?
- Will the fact that a minor seeks to place limitation on access to his or her data have to be communicated to the minor's parents or personal representative?
- Will policies addressing concerns about minors also apply to others deemed incompetent as a matter of law?

Sensitive Information

- What information will be deemed sensitive for purposes of limiting access?
- Will the requirement be based on statutory requirements such as those related to federally funded substance abuse treatment or genetic information, or will the definition be based on policy guidance such as that given by the NCVHS?

Emergency Situations

- Will HIEs incorporate "break the glass" access for emergency treatment or may a patient deny access even in an emergency circumstance?

CONCLUSION

It is clear from both state and federal law that once a patient's data is in a health information exchange, the same rules that would apply in a provider-to-provider transmittal, such as in a referral procedure, apply for transmittal of the data within the exchange. What is less clear is how patients are able to be certain that their data is protected once it is part of an HIE. Initially, decisions will have to consider a broad view of how an HIE might function, taking into account concerns of patients, providers, and other stakeholders with interests in the health care enterprise who may be focused on other issues, such as financial sustainability of an HIE or how the HIE maintains its value in improving health care generally.[87]

Beyond these threshold decisions, a number of additional questions will need to be considered. Kristin Rosati, a private attorney who has worked with several states on privacy and security issues, suggests that aspects of the core consent models might be blended. She proposed, as an example, entering all of a patient's data into an HIE with no requirement for specific consent for accessing the information for treatment purposes, but creating a separate opt-in or opt-out process for other uses such as research.[88]

The challenge for Texas HIEs will be to develop policies that encompass the capabilities of current technological management tools and anticipate evolving technology that makes data segmentation more feasible in order to ensure patients the privacy they desire, to enable providers to have access to the relevant information necessary to effectively treat patients, and to provide both patients and providers the opportunity to gain the maximum benefits from electronic health information exchange.

[87] Rosati, *supra* note 4.
[88] *Id.*